

PERTANGGUNGJAWABAN PIDANA DAN MANAJEMEN OPERASIONAL DALAM RISIKO KONSUMEN PADA PLATFORM E-COMMERCE BERBASIS AI

Apitta Fitria Rahmawati^{1*}, Yuris Tri Naili¹

¹Program Studi Hukum Program Sarjana Fakultas Ilmu Sosial Universitas Harapan Bangsa, Jl. KH. Wahid Hasyim No. 274-A, Purwokerto, 53144, Indonesia

¹apittafitriarahmawati@uhb.ac.id*, yuristrinaili@uhb.ac.id

ABSTRAK

Perkembangan pesat kecerdasan buatan (AI) pada platform e commerce membawa risiko baru bagi konsumen digital yang belum sepenuhnya dapat dijangkau oleh hukum pidana Indonesia terutama ketika keputusan algoritmik menyebabkan kerugian tanpa adanya aktor manusia yang jelas. Artikel ini menilai efektivitas hukum pidana Indonesia dalam melindungi konsumen digital serta mengevaluasi peran manajemen operasional internal seperti deteksi penipuan, perlindungan data, tata kelola algoritma dalam mitigasi risiko. Dengan metode normatif yuridis dan analisis komparatif, penelitian mengidentifikasi celah hukum terkait pertanggungjawaban pidana atas kerugian yang disebabkan oleh sistem AI (liability gap), serta menunjukkan keterbatasan kaidah mens rea dalam konteks algoritmik. Artikel ini mengusulkan model integratif yang menggabungkan reformasi aturan pidana untuk memperjelas liability korporasi dan pengembang dan standar tata kelola operasional wajib (compliance by design) untuk meningkatkan pencegahan, deteksi, dan pemulihan. Temuan menegaskan perlunya sinergi regulatif dan operasional guna memperkuat perlindungan konsumen digital di era pasar digital yang semakin otonom.

Kata kunci: AI, pertanggungjawaban pidana, e commerce, manajemen operasional, perlindungan konsumen.

ABSTRACT

The rapid development of artificial intelligence (AI) on e-commerce platforms brings new risks for digital consumers that Indonesian criminal law has not fully addressed, especially when algorithmic decisions cause harm without a clear human actor. This article assesses the effectiveness of Indonesian criminal law in protecting digital consumers and evaluates the role of internal operational management such as fraud detection, data protection, and algorithm governance in risk mitigation. Using a normative-juridical method and comparative analysis, the research identifies legal gaps regarding criminal liability for damages caused by AI systems (liability gap), and also demonstrates the limitations of the mens rea principle in the algorithmic context. This article proposes an integrative model that combines criminal rule reforms to clarify corporate and developer liability and mandatory operational governance standards (compliance by design) to enhance prevention, detection, and recovery. The findings confirm the need for regulatory and operational synergy to strengthen digital consumer protection in an increasingly autonomous digital market era.

Keywords: AI, criminal liability, e-commerce, operational management, consumer protection.

PENDAHULUAN

Perkembangan pesat teknologi Kecerdasan Buatan (AI) telah secara signifikan mengubah cara kerja berbagai industri. Kemajuan pesat dalam

teknologi AI telah mengubah cara industri berjalan, menghasilkan peningkatan efisiensi, produktivitas, serta inovasi, sejarah AI, penerapannya yang luas di berbagai sektor (Rashid & Kausik, 2024). Kemajuan teknologi kecerdasan buatan (artificial

intelligence/AI) telah mengubah cara kerja platform e-commerce dalam merancang interaksi pelanggan, mengolah data, serta meningkatkan layanan dan logistik. Penjualan produk dapat dilakukan tidak hanya secara langsung, tetapi juga melalui perantara digital (e-commerce); selain itu, pelanggan dalam e-commerce dapat berinteraksi secara aktif maupun secara pasif (Fuad, Ferdiana, & Selo, 2014).

Perkembangan kecerdasan buatan (Artificial Intelligence/AI) dalam ekosistem e-commerce tidak hanya meningkatkan efisiensi transaksi dan personalisasi layanan, tetapi juga melahirkan bentuk risiko hukum pidana yang belum sepenuhnya dapat diakomodasi oleh sistem hukum nasional. Berbeda dengan kejahatan siber konvensional yang melibatkan pelaku manusia secara langsung, penggunaan algoritma otonom berpotensi menimbulkan kerugian bagi konsumen digital tanpa keterlibatan subjek hukum yang nyata. Kondisi ini menimbulkan pertanyaan fundamental mengenai bagaimana hukum pidana Indonesia merespons kejahatan digital yang dilakukan atau dipicu oleh sistem AI secara otomatis, di tengah struktur hukum yang masih mensyaratkan adanya unsur kesalahan (mens rea) manusia sebagai pelaku yang dapat dimintai pertanggungjawaban.

Analisis sistem algoritmik yang canggih dapat menganalisis perilaku dan menerapkan deteksi penipuan yang didukung AI, seperti halnya Shopee, Tokopedia, hingga Amazon mampu menangani isu keamanan secara proaktif, yang merupakan salah satu perhatian utama konsumen saat berbelanja daring. Dalam konteks ini, fungsi AI dalam melindungi keamanan transaksi di platform juga berpengaruh langsung pada pandangan dan pengalaman pelanggan (Ainna Khansa & Tata Sutabri, 2024). Namun, dibalik adanya kemajuan yang pesat ini, memunculkan berbagai risiko yang belum sepenuhnya dapat dijangkau oleh adanya instrument hukum baik pengawasan maupun penyelesaian internal dalam suatu Perusahaan terkait.

Di zaman digital, perilaku konsumen telah berubah secara signifikan. Hal ini disebabkan oleh kemampuan teknologi yang memungkinkan perusahaan untuk berinteraksi dengan konsumen dan mencapai mereka dengan cara yang lebih efektif dan mudah. Pengguna digital saat ini menghadapi risiko pelanggaran privasi, manipulasi algoritma, pemanfaatan data pribadi, serta kejahatan siber yang memanfaatkan kecerdasan buatan secara mandiri (Natsir & Bangun, 2024). Artinya, kecerdasan buatan telah memperluas

berbagai bentuk ancaman terhadap konsumen di ranah digital, baik mulai memanipulasi algoritma hingga kejahatan siber otonom yang mengeksplorasi data pribadi sampai privasi.

Dalam konteks penerapan hukum di Indonesia, sebagaimana merupakan negara hukum yang menjamin adanya perlindungan bagi seluruh warga negaranya. Perlindungan hukum terhadap konsumen digital belum berkembang secepat dinamika teknologi digital sekarang ini. Hal tersebut menunjukkan bahwa kemajuan teknologi yang cepat membuat peraturan yang ada sering kali tidak dapat mengejar perkembangan terbaru, sehingga menciptakan celah-celah hukum (Gumilar et al., 2025). Hukum pidana nasional, baik dalam KUHP, UU ITE, UU Perlindungan Konsumen, sebagaimana hadir sebagai payung hukum namun pada dasarnya belum memiliki kerangka normative yang secara eksplisit menjangkau bentuk-bentuk kejahatan berbasis AI terutama yang terjadinya secara otomatis.

Meskipun Indonesia telah memiliki perangkat hukum seperti KUHP, UU ITE, dan UU Perlindungan Konsumen, kerangka hukum tersebut masih berorientasi pada kejahatan yang dilakukan oleh pelaku manusia dengan unsur kesalahan (mens rea) yang dapat dibuktikan. Namun, kehadiran sistem AI yang mampu mengambil keputusan secara otonom menciptakan bentuk kejahatan digital tanpa pelaku fisik yang jelas, seperti manipulasi data personalisasi harga, penipuan algoritmik, atau fraud berbasis chatbot otomatis. Hal ini memunculkan fenomena liability gap, yaitu kesenjangan pertanggungjawaban ketika kerugian terjadi akibat keputusan algoritmik tetapi tidak dapat secara langsung dikaitkan dengan niat jahat individu.

Undang-Undang Perlindungan Konsumen Nomor 8 Tahun 1999 sudah ada, peraturan ini belum secara khusus menyediakan perlindungan untuk produk digital. Dalam rangka memenuhi kebutuhan era digital, Indonesia telah mengeluarkan Peraturan Pemerintah No. 71 Tahun 2019 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik, namun pelaksanaannya masih dinilai kurang efisien dalam menangani isu perlindungan konsumen digital (Putra, Digital, & Khairun, 2024). Hal ini justru memunculkan beberapa pertanyaan fundamental yakni terkait dengan sejauh mana efektivitas hukum pidana dapat melindungi konsumen digital dari adanya risiko yang ditimbulkan oleh platform e-commerce berbasis AI.

Di sisi lain, Perusahaan e-commerce sering kali bergantung pada sistem manajemen operasional

internal untuk mengurangi risiko, termasuk dengan menerapkan sistem deteksi penipuan, pedoman etika AI, serta protokol keamanan data. Manajemen operasional meliputi perencanaan, pengorganisasian, koordinasi, serta pengawasan semua kegiatan yang terkait dengan pembuatan barang dan layanan. Dalam e-commerce, manajemen ini bertujuan untuk mengelola sumber daya secara efektif guna memproduksi barang berkualitas tinggi dengan biaya yang paling efisien (S & Serang, 2024). Namun, nyatanya efektivitas terkait dengan sistem ini sangat bergantung kepada komitmen etis dari korporasi dan tidak menutup kemungkinan untuk tidak selaras dengan standar hukum public di Indonesia. Ketidaksesuaian antara hukum pidana dan pelaksanaan manajemen risiko internal adalah tantangan utama dalam menjamin perlindungan konsumen digital secara menyeluruh.

Beragam penelitian sebelumnya lebih banyak menekankan pada aspek hukum cybercrime secara umum, atau pada regulasi perlindungan data pribadi. Di sisi lain, penelitian yang secara mendalam mengkaji hubungan antara efektivitas hukum pidana dengan sistem manajemen operasional berbasis AI dalam bidang e-commerce masih sedikit, khususnya di Indonesia. Namun, pendekatan lintas disiplin menjadi kunci untuk mengatasi kompleksitas isu hukum dan teknologi yang saling terkait dan berkembang pesat. Artikel ini bertujuan untuk mengkaji keefektifan hukum pidana dalam menangani risiko konsumen digital di platform e-commerce yang berbasis AI, serta menilai peran pengelolaan operasional perusahaan dalam mengatasi risiko-risiko ini. Studi ini juga menawarkan suatu model penggabungan antara sistem hukum dan manajemen AI internal sebagai solusi yang lebih responsif terhadap tantangan zaman digital.

Berbagai penelitian sebelumnya lebih banyak menitikberatkan pada aspek hukum perlindungan data pribadi atau cybercrime konvensional. Di tingkat internasional, kajian telah mengidentifikasi urgensi pengaturan AI berdasarkan tingkat risiko, namun belum diterjemahkan secara spesifik ke dalam konteks hukum pidana Indonesia. Dengan demikian, terdapat research gap terkait kajian eksplisit mengenai respons hukum pidana nasional terhadap liability gap akibat AI otonom dan sinergi hukum pidana dengan manajemen operasional platform.

Penelitian ini mengusulkan pendekatan lintas disiplin yang meneliti efektivitas hukum pidana dan pengelolaan operasional secara bersinergi dalam menghadapi risiko konsumen digital yang timbul

akibat penerapan teknologi kecerdasan buatan dalam platform e-commerce. Inovasi utama dari studi ini terletak pada: (1) menganalisis efektivitas hukum pidana Indonesia dalam menangani risiko konsumen digital akibat penggunaan AI dalam e-commerce. (2) Mengevaluasi peran manajemen operasional platform e-commerce dalam mitigasi risiko AI serta (3) Merumuskan model sinergi hukum pidana dan manajemen operasional dapat dibangun untuk melindungi konsumen digital.

METODE PENELITIAN

Penelitian ini menggunakan metode hukum normatif-yuridis karena fokus analisis diarahkan pada evaluasi efektivitas norma hukum positif dalam memberikan perlindungan kepada konsumen digital ketika risiko timbul akibat penggunaan kecerdasan buatan (AI) dalam platform e-commerce. Metode ini melihat hukum sebagai norma tertulis (*law in books*) dan menelaah peraturan perundang-undangan seperti KUHP, UU ITE, dan UU Perlindungan Konsumen, serta doktrin-doktrin hukum terkait pertanggungjawaban pidana. Dalam konteks preskriptif, penelitian ini menguji kecukupan norma yang ada untuk menjawab liability gap, yaitu kesenjangan pertanggungjawaban ketika keputusan algoritmik AI menimbulkan kerugian tanpa keterlibatan pelaku manusia secara langsung. Pengujian norma dilakukan melalui analisis konseptual terhadap mens rea, subjek hukum pidana, dan kemungkinan perluasan pertanggungjawaban korporasi dalam kejahatan algoritmik. Data dianalisis secara kualitatif untuk merumuskan model normatif ideal yang mampu memperkuat perlindungan konsumen digital.

HASIL DAN PEMBAHASAN

Risiko Konsumen Digital dalam Ekosistem E-Commerce Berbasis AI

Penggunaan kecerdasan buatan dalam platform e-commerce telah menimbulkan konsekuensi hukum yang tidak dapat diselesaikan secara memadai oleh kerangka hukum pidana yang berlaku saat ini di Indonesia. Hukum pidana nasional, melalui KUHP, UU ITE, dan UU Perlindungan Konsumen, masih dirancang berdasarkan paradigma tradisional di mana pelaku kejahatan selalu diasumsikan sebagai subjek hukum manusia (*natural person*) yang memiliki kemampuan bertanggung jawab serta unsur kesalahan (*mens rea*). Kondisi ini menimbulkan problematika serius ketika keputusan yang menimbulkan kerugian terhadap konsumen tidak

secara langsung dihasilkan oleh manusia, melainkan oleh sistem AI yang bekerja secara otomatis atau semi-otonom.

Konsumen digital di Indonesia semakin terpapar terhadap potensi bahaya akibat penggunaan teknologi kecerdasan buatan (AI) oleh platform e-commerce. Peningkatan kepercayaan konsumen terlihat dari bertambahnya penggunaan e-commerce oleh konsumen di seluruh dunia. Selain itu, semakin fokus pada kebijakan perlindungan konsumen dan keamanan informasi pribadi untuk menjaga keyakinan pelanggan (Utami, Irwan, & Nasution, 2023).

Di era digital yang kian maju, algoritma personalisasi tidak hanya membantu konsumen dalam mencari produk yang berkaitan, tetapi juga menimbulkan pertanyaan moral terkait privasi dan penguasaan pengguna. Algoritma personalisasi adalah sistem yang mana berbasis data untuk menyesuaikan suatu rekomendasi berdasarkan preferensi yang ada. Algoritma personalisasi, identifikasi pola belanja, serta sistem chatbot dan rekomendasi barang kini sering diterapkan untuk meningkatkan keefektifan penjualan dan efisiensi layanan. Namun, perlu diketahui bahwa dibalik semua kemudahan tersebut tentunya terdapat berbagai risiko yang signifikan khususnya dalam hal privasi, keamanan, dan keadilan informasi.

Pertama, kemunculan penipuan yang menggunakan AI adalah jenis kejahatan digital yang semakin sukar dikenali dengan cara konvensional. Sistem deteksi penipuan yang didasarkan pada kecerdasan buatan (*Artificial Intelligence*) telah muncul sebagai alternatif yang menjanjikan untuk menangani masalah ini. AI dapat menganalisis banyak data dengan cepat dan mengenali pola-pola mencurigakan yang mungkin diabaikan oleh sistem konvensional (Akbar et al., 2024). Banyak pelaku kejahatan siber memiliki kesempatan untuk mengeksplorasi teknologi untuk meniru sistem layanan yang telah tersedia resmi guna memperoleh informasi pribadi konsumen ataupun identitas privasi lainnya yang memiliki Kesan menguntungkan. Penipuan menggunakan AI ini berbeda dengan penipuan konvensional, artinya penipuan AI dapat berlangsung dalam waktu yang nyata dan sulit terdeteksi baik oleh orang ataupun sistem keamanannya yang ada.

Kedua, manipulasi algoritma yang menjadi strategi paten dalam praktik platform e-commerce. Algoritma adalah fondasi dalam pembuatan perangkat lunak, aplikasi, dan sistem computer (Hartanti, 2023). Manipulasi algoritma untuk menguasai pasar pengiriman bisa dikategorikan

sebagai sebuah bentuk penipuan dalam dunia usaha (Najlanabilla, 2025). Biasanya algoritma rekomendasi dari hasil pencarian dapat diatur bukan hanya berdasarkan relevansi obyektif, tetapi juga berdasarkan sponsor, iklan tersembunyi, bahkan berdasarkan kontrak komersial antara platform dan penjual yang terselubung. Hal tersebut akan menimbulkan pertanyaan etis sekaligus hukum mengenai apakah konsumen akan memiliki kendali serta kesadaran penuh atas informasi yang disajikan dari secara pribadi.

Ketiga, terkait dengan pengumpulan data secara berlebihan yang akan menjadikan ancaman serius terhadap hak privasi dari konsumen. Hak melindungi asasi konsumen, di Indonesia sendiri telah mereglasikan terkait dengan perlindungan tentang privasi konsumen dan perlindungan data di dalam UU ITE dan Peraturan lainnya (Natalia, Sandra, Kezia, Levina, Baasir, 2023). Berbagai platform mengumpulkan data pengguna tidak hanya selama transaksi, tetapi juga selama interaksi digital, mencakup data lokasi, perilaku klik, riwayat pencarian, bahkan durasi aktif. Profiling yang dihasilkan sering dimanfaatkan untuk segmentasi iklan atau analisis risiko kredit, tanpa adanya pemberitahuan atau persetujuan yang jelas dari pengguna.

Dalam konteks Indonesia, ketiga bentuk risiko ini belum sepenuhnya direspon oleh pemerintah melalui regulasi yang memadai. Beberapa peraturan seperti Undang-Undang Perlindungan Konsumen dan Undang-Undang Informasi dan Transaksi Elektronik belum emmiliki norma spesifik untuk menangani sistem yang cerdas secara otomatis. Hukum pidana konvensional yang mengharuskan adanya unsur mens rea sulit untuk diterapkan pada kasus kejahatan yang menggunakan algoritma, sedangkan kebijakan privasi umumnya belum mengatur pengumpulan data yang berbasis AI dengan mendetail.

Dalam KUHP dan UU ITE, pertanggungjawaban pidana hanya dapat dibebankan kepada manusia atau badan hukum yang terbukti melakukan perbuatan melawan hukum. Namun, dalam kasus kejahatan algoritmik, kesalahan tidak selalu dapat dialamatkan kepada individu tertentu, karena sistem AI dapat mengambil keputusan sendiri berdasarkan machine learning yang terus berkembang. Hal ini menyebabkan *liability gap*, yakni kesenjangan dalam menentukan siapa yang harus bertanggung jawab atas kerugian yang dihasilkan oleh keputusan algoritmik yang tidak direncanakan secara eksplisit oleh manusia.

Situasi ini menunjukkan adanya kekosongan regulasi (*regulatory gap*) dalam menangani risiko konsumen digital yang ditimbulkan oleh teknologi otonom. Dalam waktu yang sama, pemantauan terhadap platform digital masih sangat tergantung pada kebijakan internal perusahaan tanpa adanya mekanisme kontrol publik yang kuat.

Kejahatan siber konvensional (misalnya phishing manual, illegal access, carding tradisional) masih melibatkan pelaku manusia yang secara aktif melakukan tindakan melawan hukum dengan niat tertentu. Sebaliknya, kejahatan algoritmik muncul ketika sistem AI melakukan tindak yang merugikan konsumen tanpa instruksi langsung dari manusia. Contohnya termasuk diskriminasi harga otomatis berbasis profiling, penipuan oleh chatbot yang “berkembang sendiri”, manipulasi rekomendasi produk untuk eksloitasi konsumen, atau penyalahgunaan data pribadi oleh model prediktif yang tidak diawasi. Dalam konteks ini, AI dapat memosisikan diri sebagai “pemicu kerugian” tanpa adanya pelaku manusia yang eksplisit, sehingga model pertanggungjawaban pidana konvensional menjadi tidak memadai.

Dalam sistem hukum pidana Indonesia, unsur *mens rea* (niat jahat) menjadi fondasi utama dalam menentukan seseorang sebagai pelaku tindak pidana. Namun, sistem AI tidak memiliki kesadaran hukum atau kemampuan untuk memiliki niat, sehingga tidak mungkin dikenakan pertanggungjawaban pidana berdasarkan prinsip klasik. Selain itu, pembuktian hubungan kausal antara tindakan manusia (misalnya developer atau operator) dengan akibat yang ditimbulkan oleh AI sering kali tidak dapat dilakukan karena AI bertindak secara adaptif dan otonom. Akibatnya, sistem hukum saat ini tidak memiliki mekanisme yang spesifik untuk menetapkan tanggung jawab atas kerugian yang ditimbulkan oleh sistem AI.

Dalam konteks ini, penelitian ini menyuguhkan inovasi dengan membangun secara sistematis klasifikasi risiko konsumen digital yang berasal langsung dari penerapan teknologi AI dalam ekosistem *e-commerce* di Indonesia, yang masih jarang dibahas dalam penelitian hukum nasional. Risiko seperti diskriminasi algoritmik, manipulasi sistem rekomendasi, dan penipuan berbasis AI dipandang bukan hanya sebagai masalah teknologi, tetapi juga sebagai tindak kejahatan serta pelanggaran hak konsumen yang memerlukan penegakan hukum pidana dan pengelolaan digital yang lebih maju. Pemetaan ini juga menegaskan pentingnya adanya kerangka hukum yang

interdisipliner, fleksibel, dan dapat mencakup aktor non-manusia seperti sistem algoritma otonom.

Efektivitas Hukum Pidana terhadap Kejahatan Berbasis AI dalam *E-Commerce*

Perkembangan kecerdasan buatan (AI) dalam platform *e-commerce* telah melahirkan jenis kejahatan baru yang tidak selalu dapat ditempatkan dalam kategori hukum pidana konvensional. Sistem AI dapat mengambil tindakan yang merugikan konsumen secara mandiri, seperti melalui algoritma penipuan, pemrosesan data ilegal, hingga diskriminasi harga tanpa intervensi manusia langsung dalam tindakan tersebut. Situasi ini menghadirkan tantangan besar dalam konteks hukum pidana nasional yang masih berlandaskan pada model tanggung jawab individu dan kesalahan subjektif (*mens rea*).

Dalam hukum pidana Indonesia, cara menangani kejahatan digital biasanya mengacu pada Undang-Undang Informasi dan Transaksi Elektronik (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016) serta beberapa pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP). Akan tetapi, kedua regulasi tersebut belum dengan jelas mengatur aspek-aspek hukum dari aksi yang dilakukan oleh sistem otonom yang berbasis AI. Contohnya, tidak terdapat norma yang mengatur mengenai tanggung jawab pidana atas kerugian yang diakibatkan oleh keputusan algoritma yang bersifat diskriminatif, manipulatif, atau mengganggu data pribadi konsumen.

Dari ranah pidana, sistem hukum Indonesia masih berpedoman pada prinsip dasar bahwa tindak pidana merupakan perbuatan yang melawan hukum. Dalam bidang hukum terdapat istilah Perbuatan Melawan Hukum (“PMH”), yang pada dasarnya adalah tindakan yang bertentangan dengan undang-undang yang mengakibatkan kerugian, pelanggaran hukum, tindakan yang tidak sesuai dengan hak-hak orang lain, tindakan yang dilakukan di luar batas kewenangan, serta melanggar norma kesusastraan dan asas hukum umum (Auli, 2023), dimana perbuatan melawan hukum tersebut disertai dengan kesalahan dan pertanggungjawaban. Situasi ini menjadi rumit ketika sistem AI melakukan suatu tindakan tanpa adanya pengawasan langsung atau niat buruk dari pengoperasinya. Seiring dengan otonomi algoritma, semakin jauh jarak antara pelaku manusia dan konsekuensi hukum yang ditimbulkan, sehingga muncul *liability gap*.

Undang-Undang Informasi dan Transaksi Elektronik hadir sayangnya hanya bersifat administratif dan tidak memiliki daya jangkau yang

kuat terhadap kompleksitas teknologi yang lambat laun semakin kompleks seperti halnya AI. Hal ini dapat diketahui dari UU ITE pada dasarnya hanya mengatur transaksi elektronik dan informasi digital secara umum, bukan pada pembuatan konten berbasis algoritma yang secara mandiri dilakukan oleh mesin. Saat AI dapat membuat keputusan atau menghasilkan karya tanpa interaksi manusia secara langsung, metode hukum konvensional menjadi tidak berlaku (Arbani, 2025). Akibat yang ada, banyak nantinya kasus penipuan digital berbasis AI yang tidak diproses secara efektif karena penegak hukum kesulitan dalam pembuktian unsur subjektif dan identifikasi pelakunya.

Kekosongan kerangka hukum pidana yang teknologi serta responsive juga terlihat dari belum adanya mekanisme hukum untuk ranah teknologi digital yang saat ini. Sistem hukum pidana Indonesia yang berlandaskan territorial tidak cukup efektif dalam menghadapi kejahatan digital yang bersifat transnasional. Selain itu, banyak norma hukum pidana yang berlaku saat ini masih berfokus pada jenis kejahatan fisik, sehingga belum dapat menampung kompleksitas tindakan kriminal yang terjadi di dunia maya (Syahputra, 2025). Banyak negara maju sudah mengenai posisi hukum AI, Uni Eropa telah mengesahkan undang-undang AI yang menyeluruh yang mengatur pemanfaatan AI. Peraturan itu dikenal sebagai European Union Artificial Intelligence Act 2024 ("AIA 2024"). AIA 2024 memiliki tujuan untuk menjamin bahwa AI diterapkan dengan aman, transparan, dan bertanggung jawab, serta untuk meminimalkan risiko yang mungkin muncul dari penggunaannya, seperti bias atau diskriminasi (Ramlil, 2024) sementara Indonesia masih berada pada tahap awal dirkusus tersebut, meskipun secara umumnya telah terdapat RUU terkait dengan Perlindungan Data Pribadi yang sebagiannya sudah menyentuh isu pemrosesan otomatisasi data, tetapi saja masih belum memiliki kerangka hukum pidana yang teknologi serta responsive.

Fakta ini mengindikasikan bahwa pendekatan hukum pidana di Indonesia terhadap kejahatan digital, terutama yang melibatkan teknologi AI, masih bersifat terputus-putus, reaktif, dan belum disesuaikan dengan sifat risiko teknologi otonom. Namun, pentingnya pembaruan ini semakin meningkat seiring dengan bertambahnya penggunaan AI dalam layanan publik digital, termasuk dalam *e-commerce*.

Kebaruan utama dari penelitian ini terletak pada penemuan batasan mendasar dalam sistem hukum pidana Indonesia yang belum dapat mencakup

entitas non-manusia seperti sistem kecerdasan buatan (AI) yang bersifat mandiri. Pendekatan hukum pidana yang selama ini berfokus pada elemen mens rea dan tanggung jawab individu menjadi kurang memadai dalam menangani kejahatan digital yang dipengaruhi oleh algoritma. Penelitian ini memberikan pandangan baru bahwa regulasi AI seharusnya tidak hanya diletakkan dalam konteks perlindungan data pribadi atau aspek administratif saja, tetapi juga harus diintegrasikan ke dalam sistem hukum pidana sebagai bentuk perlindungan substantif bagi konsumen digital. Artikel ini juga mengusulkan perlunya peninjauan kembali pertanggungjawaban pidana yang berlandaskan struktur institusi, dengan menekankan pada kegagalan manajemen perusahaan dalam mengatur dan mengawasi sistem AI yang mereka kelola. Pandangan ini memperluas ruang lingkup diskursus hukum pidana di Indonesia yang selama ini belum secara jelas mengkaji tanggung jawab perusahaan terhadap risiko algoritmik yang merugikan konsumen.

Peran Manajemen Operasional Platform dalam Mitigasi Risiko Konsumen

Dalam konteks *e-commerce* berbasis kecerdasan buatan (AI), Manajemen operasional memiliki peran krusial dalam bisnis digital sebab bertanggung jawab untuk memantau dan mengatur kegiatan produksi. Dalam bisnis digital, aspek-aspek seperti keuangan, pemasaran, dan produksi perlu dipantau secara teliti supaya operasional berjalan dengan baik. Inti dari manajemen operasional adalah merancang dan melaksanakan aktivitas bisnis, memastikan bahwa proses produksi berjalan sesuai dengan tujuan, serta mendukung pencapaian sasaran Perusahaan (Wahono, Puji ; Usman, Osly ; Afiyah, 2021).

Ketiadaan pengaturan eksplisit mengenai perbuatan melawan hukum yang dilakukan oleh sistem AI menuntut lahirnya konstruksi baru dalam hukum pidana Indonesia. Dalam konteks kejahatan algoritmik, pertanggungjawaban pidana tidak lagi dapat sepenuhnya bertumpu pada pelaku manusia individual, melainkan harus dialihkan pada entitas yang memiliki kontrol dan tanggung jawab atas sistem AI tersebut. Oleh karena itu, pendekatan *corporate criminal liability* (pertanggungjawaban pidana korporasi) menjadi salah satu opsi yang relevan, di mana pengembang, penyedia platform *e-commerce*, atau entitas yang memperoleh keuntungan dari penggunaan AI dapat dimintai pertanggungjawaban atas risiko algoritmik yang merugikan konsumen.

Dalam kasus di mana unsur kesalahan (mens rea) sulit dibuktikan karena AI bekerja secara otomatis, penerapan strict liability dapat dipertimbangkan, yaitu pertanggungjawaban pidana yang tidak mensyaratkan pembuktian unsur niat jahat. Model ini lebih menitikberatkan pada aspek risiko (risk-based liability) dari penggunaan teknologi AI oleh pelaku usaha digital. Dengan demikian, pihak yang menggunakan AI sebagai bagian dari sistem operasional wajib memastikan bahwa teknologi tersebut tidak menimbulkan kerugian bagi konsumen, dan setiap pelanggaran yang terjadi menjadi tanggung jawab hukum mereka secara langsung.

Manajemen operasional platform juga memegang peran sentral dalam mitigasi risiko yang dihadapi oleh konsumen digital. Risiko-risiko tersebut meliputi pencurian informasi pribadi, manipulasi algoritma, bias sistemik dalam saran produk, serta kemungkinan penipuan yang dilakukan melalui otomatisasi yang didorong AI. Oleh sebab itu, sistem manajemen operasional yang responsif dan adaptif bukan hanya merupakan kebutuhan teknis, tetapi juga sebagai dasar etika dan hukum dalam melindungi konsumen.

Manajemen operasional pada platform digital melibatkan serangkaian proses yang mencakup desain sistem, pengelolaan infrastruktur teknologi, kebijakan pengawasan data, serta pengendalian mutu interaksi pengguna. Dalam praktiknya, aspek ini berkaitan langsung dengan penerapan prinsip privacy by design, tanggung jawab algoritmik, dan tata kelola AI yang etis yang mulai diadopsi oleh beragam platform global. Selayaknya dalam teori pelaksanaan kebijakan yang dirumuskan oleh Mazmanian dan Paul Sabatier, salah satu aspek penting yang mempengaruhi keberhasilan implementasi kebijakan adalah sifat dari masalah yang dihadapi. Istilah ini menyangkut seberapa efektif suatu masalah dapat diselesaikan melalui kebijakan publik. Beberapa faktor yang memengaruhi karakteristik tersebut meliputi kompleksitas teknis, variasi dan jumlah pihak yang dituju oleh kebijakan, serta tingkat pengaruh pembuat kebijakan terhadap perilaku kelompok yang menjadi target (Radiani & Monalisa, 2025).

Salah satu dimensi penting dalam mitigasi risiko konsumen adalah kemampuan dari platform untuk membangun sistem deteksi dini terhadap perilaku yang algoritmik berpola menyimpang. Selain itu, transparansi dalam operasi merupakan elemen penting untuk menciptakan akuntabilitas platform. Konsumen digital saat ini mengharapkan transparansi mengenai proses data mereka, sejauh

mana keputusan otomatis memengaruhi pilihan belanja, dan apa saja langkah perbaikan yang ada ketika sistem mengalami kegagalan. Manajemen operasional yang menggabungkan prinsip explainable AI (XAI) dan tata kelola yang berfokus pada konsumen tidak hanya memperkuat daya tawar konsumen, tetapi juga mengurangi risiko litigasi yang bisa merugikan platform dari segi reputasi dan finansial.

Kesuksesan mitigasi risiko bagi konsumen lewat manajemen operasional sangat bergantung pada penggabungan antara sistem teknologi dan ketentuan hukum internal platform. Praktik terbaik menunjukkan bahwa kolaborasi antara divisi hukum dan operasional akan menciptakan pendekatan pencegahan yang lebih efisien dibandingkan hanya bereaksi terhadap pelanggaran yang sudah berlangsung. Dalam kerangka ini, platform sebaiknya membentuk unit kepatuhan yang beroperasi secara lintas disiplin melibatkan pakar AI, ahli hukum siber, dan manajer risiko untuk terus-menerus mengevaluasi dan memperbarui protokol operasional sesuai dengan perkembangan teknologi dan regulasi.

Oleh karena itu, manajemen operasional di platform e-commerce yang berbasis AI bukan hanya sekadar fungsi administratif, tetapi juga alat strategis dalam menjaga perlindungan konsumen digital. Apabila pendekatan ini diterapkan secara sistemik dan berlandaskan prinsip kehati-hatian, maka efektivitas hukum pidana sebagai upaya terakhir dapat menurun. Dengan kata lain, keberhasilan pengelolaan risiko melalui manajemen operasional juga membantu efisiensi hukum, mengurangi beban pembuktian dalam kasus pidana digital, serta mendorong terbentuknya ekosistem e-commerce yang adil dan berkelanjutan.

Dalam konteks ini, manajemen operasional platform tidak hanya dipandang sebagai sistem teknis internal, tetapi juga sebagai bentuk pelaksanaan kewajiban hukum preventif. Konsep compliance by design dan algorithmic accountability harus diposisikan sebagai wujud tanggung jawab hukum korporasi dalam memastikan sistem AI yang digunakan tidak menimbulkan kerugian terhadap konsumen digital. Dengan demikian, efektivitas hukum pidana hanya akan optimal apabila didukung oleh mekanisme pengawasan internal platform yang mampu mendeteksi, mencegah, dan mengoreksi penyimpangan AI sejak tahap perancangan.

Sinergi antara Hukum Pidana dan Manajemen Operasional Menuju Perlindungan Konsumen Digital yang Efektif

Berdasarkan analisis sebelumnya, efektivitas perlindungan konsumen digital dalam ekosistem e-commerce berbasis AI tidak dapat hanya mengandalkan penegakan hukum pidana secara represif. Hukum pidana akan sulit bekerja jika tidak didukung oleh sistem internal platform yang mampu mendeteksi, melacak, dan mengendalikan risiko algoritmik. Oleh karena itu, diperlukan sinergi antara konstruksi baru pertanggungjawaban pidana dengan manajemen operasional platform sebagai bentuk pertanggungjawaban preventif.

Perlindungan konsumen dalam platform e-commerce yang menggunakan kecerdasan buatan (AI) perlu pendekatan multidisipliner yang tidak bisa ditangani secara terpisah. Hukum pidana, yang selama ini dianggap sebagai alat untuk menghukum pelanggaran hak konsumen, semakin menghadapi tantangan dalam konteks digital karena sifat pelaku, objek, dan cara pelanggarannya yang tidak biasa. Sebaliknya, manajemen operasional platform sebenarnya merupakan entitas yang memiliki kontrol sepenuhnya atas infrastruktur risiko baik melalui pengelolaan sistem AI, pengumpulan dan pengolahan data, maupun pengaturan perilaku pengguna dalam ekosistem digital. Oleh karena itu, yang diperlukan bukanlah dominasi satu pendekatan, melainkan kolaborasi fungsional antara hukum pidana dan manajemen operasional dalam menciptakan sistem perlindungan konsumen yang efisien, pencegahan efektif, dan responsif terhadap perubahan teknologi.

Pendekatan hukum pidana yang efisien di era digital tidak hanya harus menanggapi pelanggaran yang telah terjadi, tetapi juga perlu merancang mekanisme pencegahan yang sistematis yang terintegrasi dalam operasi teknologi platform. Di sinilah posisi penting dari kolaborasi tersebut. Contohnya, pada situasi manipulasi algoritmik yang mengakibatkan eksploitasi preferensi konsumen secara tidak kasat mata, pembuktian pidana menjadi rumit karena ketiadaan jejak mens rea individu yang tegas. Namun, apabila manajemen operasional melaksanakan audit algoritmik secara berkala, menerapkan catatan transparansi, serta membentuk unit kepatuhan etika AI, maka kemungkinan pelanggaran dapat diidentifikasi dan diatasi sebelum bertransformasi menjadi masalah hukum.

Dalam konteks hukum pidana, adanya mekanisme mitigatif dalam fungsi platform dapat dimanfaatkan sebagai indikator tanggung jawab korporasi atau pengelola sistem. Hal ini memberikan kesempatan untuk menerapkan tanggung jawab berbasis kelalaian dalam kejahatan

sistem, yaitu ketika pengelola tidak memperhatikan pembangunan pengelolaan operasional yang cukup, sehingga mengakibatkan kerugian bagi konsumen. Dengan kata lain, efektivitas hukum pidana ditingkatkan tidak hanya melalui perluasan delik, tetapi juga dengan mengontekstualisasikan norma pidana dalam hubungan teknis antara manusia dan sistem AI.

Sebaliknya, manajemen operasional pun memperoleh keuntungan dari kerangka hukum pidana yang berfungsi sebagai batas normatif. Kriteria minimum yang ditentukan oleh undang-undang dapat dijadikan acuan dalam merancang protokol keamanan, sistem pelaporan kejadian, dan pelatihan staf teknis. Hal ini krusial untuk menghindari bias desain yang mengesampingkan hak konsumen terkait privasi, keamanan data, dan keadilan algoritmik. Melalui kolaborasi antara regulator dan penyedia teknologi, usaha perlindungan konsumen akan beralih dari pendekatan yang berlandaskan kepatuhan menuju pendekatan yang mengedepankan kepercayaan dan transparansi.

Kebaruan utama yang dihadirkan dalam kajian ini adalah penggabungan secara konseptual dan fungsional antara hukum pidana serta manajemen operasional dalam konteks perlindungan konsumen digital yang didasarkan pada AI. Studi sebelumnya seringkali memisahkan fungsi hukum sebagai sarana hukuman dan fungsi manajemen sebagai proses teknis internal, sehingga menimbulkan kekurangan perlindungan di ruang digital. Artikel ini mengajukan model interaktif-hibrid, di mana hukum pidana tidak hanya berperan sebagai mekanisme terakhir (*ultima ratio*), tetapi juga sebagai elemen dari *risk governance* dalam pengelolaan operasional platform. Dengan menciptakan kerangka kerja kolaboratif antara peraturan hukum dan mekanisme operasional, perlindungan konsumen tidak hanya tergantung pada tindakan, tetapi pada daya sistem untuk mencegah, mendeteksi, dan memperbaiki pelanggaran secara internal dan berkesinambungan.

Oleh karena itu, penanganan risiko konsumen digital akibat penggunaan AI dalam platform e-commerce membutuhkan model pertanggungjawaban pidana yang adaptif dan berbasis pada kontrol risiko. Model tersebut harus diintegrasikan dengan tata kelola manajemen operasional platform yang mendukung accountability AI secara preventif. Sinergi antara keduanya menjadi dasar pembentukan model perlindungan konsumen digital yang lebih efektif di tengah semakin kompleksnya kejahatan algoritmik.

I. SIMPULAN

Penelitian ini menunjukkan bahwa sistem hukum pidana Indonesia saat ini belum memiliki mekanisme yang memadai untuk mengatur pertanggungjawaban terhadap kejahatan yang dilakukan oleh kecerdasan buatan (AI) yang bekerja secara otonom tanpa subjek hukum manusia yang jelas. KUHP dan UU ITE masih mensyaratkan adanya pelaku manusia sebagai subjek hukum yang memiliki kesalahan (mens rea), sehingga muncul liability gap ketika kerugian konsumen digital timbul akibat keputusan algoritmik AI yang tidak dapat dikaitkan secara langsung dengan niat jahat individu tertentu.

Kondisi ini membedakan kejahatan algoritmik dari kejahatan siber konvensional, karena yang pertama bersifat *non-anthropocentric* dan bergantung pada sistem teknologi yang bertindak secara adaptif. Oleh karena itu, sistem hukum pidana Indonesia memerlukan rekonstruksi paradigma pertanggungjawaban melalui perluasan subjek hukum dan penerapan model baru criminal liability yang lebih sesuai dengan karakteristik teknologi AI, seperti *corporate criminal liability*, *strict liability*, *risk-based liability*, atau *vicarious liability* terhadap korporasi pengendali sistem AI.

Selain itu, perlindungan konsumen digital tidak dapat bergantung pada penegakan hukum pidana yang bersifat represif saja, tetapi harus diintegrasikan dengan manajemen operasional platform yang menerapkan prinsip *compliance by design*, *algorithmic accountability*, dan pengawasan manusia (*human oversight*). Dengan demikian, sinergi antara pembaruan konstruksi hukum pidana dan penguatan tata kelola AI dalam operasional *e-commerce* merupakan model ideal untuk membangun sistem perlindungan konsumen digital yang adaptif dan responsif terhadap perkembangan teknologi kecerdasan buatan.

SARAN

Sebagai rekomendasi, pembentukan regulasi khusus mengenai kejahatan berbasis kecerdasan buatan perlu menjadi prioritas bagi pembentukan undang-undang (DPR dan Pemerintah). Hal ini dapat diwujudkan melalui penambahan bab khusus dalam KUHP atau penyusunan undang-undang tersendiri terkait tindak pidana berbasis AI yang mengatur kategori kejahatan algoritmik, klasifikasi perbuatan melawan hukum berbasis teknologi, serta penetapan model pertanggungjawaban pidana yang tidak lagi bergantung pada eksistensi pelaku

manusia secara langsung. Dalam kerangka ini, diperlukan pula rekonstruksi konsep pertanggungjawaban pidana melalui penerapan model *corporate criminal liability*, *strict liability*, *vicarious liability*, atau *risk-based liability*, sehingga entitas yang mengendalikan dan memperoleh manfaat dari penggunaan AI seperti korporasi, platform *e-commerce*, maupun pengembang sistem dapat dimintai tanggung jawab hukum secara proporsional.

Bagi penegak hukum (penyidik, jaksa, dan hakim), diperlukan pedoman interpretatif yang progresif untuk mengidentifikasi bentuk kelalaian teknologi (*technological negligence*) serta menetapkan kriteria subjek hukum yang dapat dimintai pertanggungjawaban atas kejahatan algoritmik. Pada saat yang sama, regulator digital dan otoritas sektor (seperti Kominfo, OJK, dan BI) perlu mengembangkan standar tata kelola AI nasional melalui mekanisme audit algoritmik, sertifikasi keamanan teknologi, pengawasan berbasis risiko, serta kewajiban penerapan prinsip *compliance by design* dan *algorithmic accountability*. Selain itu, bagi pelaku usaha digital dan penyelenggara platform *e-commerce*, sistem manajemen operasional harus diarahkan pada penerapan *algorithmic transparency*, *human oversight*, serta mekanisme remediasi otomatis yang mampu mencegah timbulnya kerugian konsumen sejak tahap awal. Untuk mendukung seluruh agenda tersebut, komunitas akademik dan pusat penelitian hukum pidana perlu mengembangkan pemikiran teoretis yang lebih adaptif terhadap perkembangan teknologi digital sekaligus menyusun model konseptual yang dapat menjadi landasan bagi pembaruan hukum pidana berbasis kecerdasan buatan di Indonesia.

DAFTAR PUSTAKA

- Ainna Khansa, & Tata Sutabri. (2024). Pengembangan Customer Experience Berbasis Artificial Intelligence pada Startup Marketplace Shopee. *Router: Jurnal Teknik Informatika Dan Terapan*, 2(4), 28–39. <https://doi.org/10.62951/router.v2i4.270>
- Akbar, M. R., Hidayatullah, K. M. S., Sutabri, T., Informatika, P. T., Teknik, F., & Darma, U. B. (2024). Untuk Meningkatkan Keamanan Transaksi Pada. 10(02), 10107–10111.
- Arbani, M. (2025). Kekosongan Hukum Artificial Intelligence di RI: Ancaman & Tantangan.
- Auli, R. C. (2023). Perbedaan Perbuatan Melawan Hukum dalam Hukum Perdata dan Pidana. Retrieved July 14, 2025, from Hukum Online

- website:
<https://www.hukumonline.com/klinik/a/perbedaan-perbuatan-melawan-hukum-dalam-hukum-perdata-dan-pidana-lt5142a15699512/>
- Fuad, E., Ferdiana, R., & Selo. (2014). Perancangan Fitur E-Commerce Berdasarkan Konsep Customer Relationship Management Untuk Meningkatkan Kualitas Pelayanan. *Prosiding SNATIF Ke-1*, 259–266.
- Gumilar, E. R., Sitanggang, M. J., Remal, S., Ketaren, A., Everoes, M. E., Nasional, P., ... Journal, F. L. (2025). *Rekonstruksi Penyelesaian Sengketa Perlindungan Konsumen pada Pihak Ketiga sebagai Upaya Transformasi Ekonomi Digital Reconstruction of Consumer Protection Dispute Resolution Involving Third Parties as a Measure to Advance Digital Economic Transformation*. 2(1), 15–28.
- Hartanti, T. (2023). Pengaruh Penerapan Algoritma Pemrograman Pada Kurikulum Merdeka. 01(03), 76–79.
- Najlanabilla, A. (2025). *Praktik Ihtikar dalam E-commerce : Tinjauan Kasus Dugaan Monopoli Shopee dari Perspektif Ekonomi Islam*. 4, 3546–3553.
- Natalia, Sandra, Kezia, Levina, Baasir, H. N. (2023). Privasi Konsumen Dan Perlindungan Data: Prespektif Kebijakan Dan Studi Perbandingan. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 10(6), 3157–3168.
- Natsir, K., & Bangun, N. (2024). *Strategi UMKM Menghadapi Perubahan Perilaku Konsumen Di Era Digital Teknologi untuk menjalankan bisnis mereka . Selain itu pelaku UMKM juga harus memahami*. 2(3), 772–777.
- Putra, G. P., Digital, P., & Khairun, U. (2024). *Permasalahan Hukum dalam Perlindungan Konsumen terhadap Produk Digital : Tantangan dan Solusi di Era E- Commerce*. (November), 1–10.
- Radiani, R., & Monalisa. (2025). Efektivitas Pelayanan Perizinan Sistem Online Single Submission (OSS) Oleh Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu Kota Pekanbaru. *JMP: Jurnal Mahasiswa Pemerintahan*, 2(2), 210–215.
- Ramli, A. M. (2024). Artificial Intelligence (AI): Subjek Hukum atau Objek Hukum? Retrieved July 14, 2025, from Hukum Online website:
<https://www.hukumonline.com/klinik/a/ai-subjek-hukum-atau-objek-hukum-lt670eca701fc74/>
- Rashid, A. Bin, & Kausik, M. A. K. (2024). AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. *Hybrid Advances*, 7(August), 100277.
<https://doi.org/10.1016/j.hybadv.2024.100277>
- S, R. A. P., & Serang, S. (2024). *Analisis Model Bisnis dan Manajemen Operasional Perusahaan Start-up*. 5(12), 5954–5963.
- Syahputra, M. D. (2025). Dinamika Hukum Pidana Dalam Menanggapi Kejahatan Siber Di Era Digital. *Jurnal Ilmiah Multidisiplin Terpadu*, 9(5), 149–154.
- Utami, A., Irwan, M., & Nasution. (2023). Perkembangan Pasar Online (E-Commerce) Di Era Modern Dan Pengaruhnya Terhadap Kepercayaan Konsumen. *Jurnal Ekonomi Manajemen Dan Bisnis*, 1(2), 126–132.
- Wahono, Puji ; Usman, Osly ; Afiyah, M. E. (2021). *Manajemen Bisnis Digital Strategi dan Praktik untuk Generasi Digital*.